AIR COMMAND AND STAFF COLLEGE

DISTANCE LEARNING

AIR UNIVERSITY

CYBER WARFARE GOVERNANCE: EVALUATION OF CURRENT INTERNATIONAL AGREEMENTS ON THE OFFENSIVE USE OF CYBER

By

Nicholas Lewis, DAF

Muir S. Fairchild Research Information Center
Digital Collections
Air University–Maxwell AFB, AL

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Proposal Adviser: Dr. Brett Morris

Project Adviser: Dr. Andrew Niesiobedzki

Maxwell AFB, AL

October 2015

DISTRIBUTION A. Approved for public release: distribution unlimited.

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Air University Eaker Center Fairchild Research Information Center Digital Collections Air University–Maxwell AFB, AL

Table of Contents

Disclaimer ii

Table of Contents iii

List of Figures iv

Abstract v

Overview 1

Nature of the Problem 2

Purpose of the Study 4

Research Question 4

Research Methodology 5

Literature Review 6

General Warfare Documents 6

Conflict Case Studies and Reports 7

Current International Cyber Agreements 12

Analysis, Conclusions and Recommendations 20

Analysis 20

Conclusions 26

Recommendation 28

Notes 29

References 31

Digital Collections

List of Figures

Figure 1: Illustration of the how STUXNET performs 10

Muir S. Fairchild Research Information Center
Digital Collections
Air University–Maxwell AFB, AL

Abstract

The increased use of cyberspace on the battlefield has begun to blur the lines of what was understood to be acceptable according to the current warfare guidance. This research will evaluate the effectiveness of the current guidance as well as other documents that are currently available in order to determine if the nuances that cyber operations bring to the battlespace are accurately covered. The primary documents examined in this research are the Geneva Convention and all of its additional protocols, the Tallinn Manual published by the NATO Cooperative Cyber Center of Excellence, and the United Nations publication on acceptable behaviors in cyberspace. Case studies on the Russian attacks on Georgia and Estonia, the STUXNET attacks on Iran and the recent OPM hacks by Chinese actors will examined to prove the need for documentation that can direct apply international law to the cyber domain. After analysis of the effectiveness of the guidance documents when applied to the situations when cyber operations were carried out, the recommended course of action was to lobby for the adoption of the Tallinn Manual as the comprehensive guidance for wartime using current technologies. The Tallinn Manual provides the same guidance as the Geneva Convention but includes expanded definitions to include cyber related scenarios, making it great candidate for the first international agreement to apply the tenets of *Jus in Bello* and *Jus as Bellum* to cyberspace.

Air University Fairchild Research Information Center Digital Collections Air University–Maxwell AFB, AL

INTRODUCTION

Overview

Attempts at international agreements over the military use of cyberspace have been a reoccurring situation over the past 10-20 years. Russia, China, and the United States as well as other countries all believe that there should be some kind of regulatory agreement on how cyberspace can be used as a military capability. Dating back to 1998 the United States and Russia have been two of the primary nations involved in these talks and they have continuously failed to come to a common understanding on the use of cyber within the military. There have been proposed agreements on cyber security, international law enforcement in regards to cyber and restrictions on offensive cyber capabilities, but for the purpose of this research the focus will be on an agreement that outlines the acceptable use of state or state sponsored title 10 cyber capabilities in war.

Digital Collections

In regards to cyber, the U.S. has historically taken a defensive stance while Russia and China have favored an agreement that limited state sponsored offensive capabilities.[1]This difference in views has shown itself to be the primary hurdle in reaching an agreement that would be mutually beneficial to all parties. The current administration's view on cyberspace still focuses on defensive measures within cyberspace and very rarely mentions anything that would be considered an offensive act in the cyber domain. President Obama's priorities have been identified as "protecting the country's critical infrastructure, improve our ability to identify and report cyber incidents, engage with international partners to promote internet freedom, securing federal networks and shaping a cyber-savvy workforce integrating more with the private sector.[2]" While all of these priorities are defensive in nature, they could still be achieved with an agreement that includes the limitation of offensive capabilities. With the increased roles and

capabilities of U.S. Cyber Command, the Unites States' use of Title 10 cyber capabilities is likely to increase which could trigger another arms race with our adversaries in the cyber domain, if acceptable operating procedures in the cyber domain are not identified.

Currently, different aspects of the military use of cyber may be covered under existing treaties or agreements but due to the uniqueness of the cyber domain an overarching agreement with a common language is likely necessary. Russian military cyber-attacks against Estonia and Georgia targeted critical infrastructure that prevented civilian population centers from using telecommunication networks that were required to call emergency services and receive emergency information. The use of cyber was coordinated with Russian traditional military attacks and provided a force multiplier that had not previously been seen[34]. If left unchecked countries will continue to exploit the vulnerabilities inherent in the worldwide telecommunication networks regardless of its effect on the civilian population. In early May 2015, the Russians and Chinese agreed to a cyber non-aggression agreement between the two nations. Russia's previous use of military cyber and their new ties with China may be signaling that we are beyond the point of worrying about independent hackers and that state sponsored cyber is to the point where it needs to be regulated. The lack of a recognized international agreement will potentially cause a cyber arms race and as capabilities evolve cyber could become one of the next WMDs.

Nature of the Problem

An international agreement on the military use of offensive cyber capabilities is necessary to ensure that all of the unique attributes of the cyber domain are addressed with language specific to the technology as well as to establish a common legal interpretation between

nations. Throughout history war has been an unwanted but sometimes necessary part of life. In order to ensure that both combatants and non-combatants retain their basic human rights and are not subject to inhumane treatment the international community developed standards of war in the form of a treaty. Treaties such as the Geneva Convention identify that "civilian objects shall not be the object of attack or reprisal" and that "works or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, shall not be made the object of an attack, even where these objects are military objectives"[56]. While these rules were initially written well before cyberspace had a role in warfare, their wording is so vague that it could still hold true for cyber. In recent years there have been threats against civilian communication systems, financial institutions and even cyber-attacks on a nuclear facility in the form of the STUXNET virus[7]. Those threats appear to directly violate the agreements within the Geneva Convention identified above; however they are not treated as a violation of international law.

For years other nations have pushed for an international agreement on the use of offensive cyber and the United States. Has pushed back saying that an agreement was unnecessary and that those nations were trying to use such agreements to further their own agendas[8]. However as more and more nations develop their own capabilities and cyber policies, the legal interpretation of how traditional warfare agreements such as the Geneva Conventions apply to cyber is beginning to vary widely. Actions that the U.S. may deem illegal due to Law of Armed Conflict (LOAC) concerns may be perfectly acceptable to other nations and this begins to create a level of ambiguity within the international community. To further add to the need for an international agreement, nations such as China and Russia have begun signing their own cyber non-aggression agreements which will allow them to focus the use of cyber against other

Digital Collections
Air University, Maxwell AFB, AL

adversarial nations using their own recognized language which is not in accordance with the rest of the international community[9].

Purpose of the Study

The purpose of this study is to evaluate current legal agreements and treaties between nations adequately cover the use of offensive cyber capabilities, primarily against civilians or civilian infrastructure. Documents such as the Geneva Convention and the Hague Conventions are worded in a way that they can be applied to almost every facet of war. The latest versions of those documents were written decades ago yet they still heavily dictate the way that most countries in the world approach warfare. While those documents were written in a manner that the terminology could be interpreted in multiple different ways, they were written in a time where warfare was fought between two opposing forces that met on a battlefield. With the introduction of the cyber domain, the above statement no longer holds true. Cyber is a man-made domain that essentially stretches the battlefield worldwide. It has begun to blur the lines of what we have traditionally determined the battlespace to be. Therefore the purpose of this study is to evaluate the effectiveness of current international legal agreements and treaties as they relate to this new expanded battlespace.

Research Question

As warfare continues to evolve with technology, the use of cyber capabilities in offensive operations will increase. It provides commanders with an option that is sometimes repeatable, reversible cheaper, and does not require human lives to be put in harm's way. The world has already begun to see examples of how when used effectively, cyber can become a force multiplier that dramatically increases someone's chance of success. While cyber capabilities can

provide real world effects in the air, land, sea and space domains, it is primarily executed within the cyberspace domain. The cyberspace domain is the first manmade domain and it does not rely on the same physical boundaries and constraints that the other domains have to abide by. Therefore the research question for this study is; how effective are the current international legal agreements and treaties at covering all of the nuances that cyberspace and offensive cyber capabilities bring to the battlespace?

Research Methodology

This research will utilize an evaluative framework to establish the effectiveness of the current international agreements and treaties during times when offensive cyber capabilities were used during conflicts. The evaluation will consider the target of the capability in relation to the actual equipment that was affected, the affect that the capabilities had on the civilian population, and whether or not the capability used would be considered a Title 10 effect at the time of execution or in the near future. The intent will be to apply sections of legal documents such as the Geneva Conventions and the Law of Armed conflict to situations that occurred in the Russia-Estonia conflict, Russia-Georgia conflict, the STUXNET attack against the Iranian nuclear facilities, and the recent hacking of multiple United States information systems by the Chinese. The different circumstances within each of those conflicts will apply to different sections of the legal documents and will provide a more comprehensive answer as to how effective those documents can be at regulating the use offensive cyber capabilities.

Digital Collections

Literature Review

Almost all of the resources used within this paper fall into one of two categories; international agreements on general warfare or case studies on conflicts where offensive cyber capabilities were used. While the documentation regarding general warfare documents such as the Geneva Convention and Law of Armed Conflict interpretations have been around for decades, the bulk of the offensive cyber activity has been relatively recent. Due to some of the situations regarding the use of cyber occurring within the past year, multiple secondary and tertiary references will have to be used to describe those situations in the absence of primary references.

General Warfare Documents

The warfare documents that detail the general rules of war will provide the primary information that will be evaluated. An in-depth understanding of these documents will be required to accurately evaluate their effectiveness when it comes to the use of cyber. The primary document for the baseline will be the Protocol Additions to the Geneva Convention, specifically Protocol 1. Article 52 of Protocol 1 deals with the "General Protection of Civilian Objects" and contains the definition of what constitutes a civilian object; "civilian objects shall not be the object of attack or of reprisals. Civilian objects are all objects which are not military objectives."[10] Article 52 of Protocol 1 goes on to define military objectives as "objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a military advantage" and "in case of doubt whether an object which is normally dedicated to civilian purposes, such as a place of worship, a house or other dwelling or a school, is being used to make an effective contribution to military action, it shall be presumed not to be so

used.[11]" In addition to the definitions of protected civilian objects, Protocol 1 also defines "Protection of works and installations containing dangerous forces"[12]. Article 56 states:

> "Works or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, shall not be made the object of attack, even where these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civil population."

And "the special protection against attack shall cease for a nuclear electrical generating station only if it provides power in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support.[13]" These definitions are important to understand because they set the precedent and guidelines for how the international community is to approach warfare.

In addition to the Geneva Convention, a U.S. Army Judge Advocate General's Legal Center and School interpretation of the Law of Armed Conflict is used to help supplement the definitions within the Geneva conventions with United States legal interpretations. The *Law of Armed Conflict Deskbook* incorporates information from the Geneva Convention and its additional protocols, The Hague Conventions, and Unites States service manuals and handbooks to show where the U.S. legal interpretations of war were derived[14].

Conflict Case Studies and Reports

This research paper will focus on the application of the general warfare documents identified above to five different conflicts where offensive cyber capabilities were used. The five conflicts consist of the Russia-Estonia conflict, Russia-Georgia conflict, the STUXNET attack against the Iranian nuclear facilities, and the recent hacking of multiple United States information systems by the Chinese. The Russia-Estonia conflict in 2007 was one of the first cases where offensive cyber capabilities were used with a high level of success. In Stephen

Herzog's article in the Journal of Strategic Studies, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses" he outlines the importance of the attacks on Estonia. At the time of the attacks Estonia was one of the most "wired" or "networked" countries in the world and Russia proved that they were able to completely negate that technology using a massive denial of service attack[15]. Russian hackers were able to cripple the Estonian banking systems, disable parliamentary email servers and denied government ministry IT systems connectivity to national networks. The effect of the attacks were so successful that an Estonian defense representative compared the attacks to a successful blockade of all of a country's naval ports[16]. Herzog uses the success of the attacks to point out that the globalization of the internet will require multinational agreements in order to effectively defend individual nations' networks. This forced the world to realize that while the global interconnectivity of networks and our reliance on technology for systems such as supervisory control and data acquisition, finance systems, telecommunication systems and even military weapon systems are now vulnerable to this type of attack[17].

Digital Collections
Air University–Maxwell AFB, AL

One year after the Russian attacks on Estonia, the Russians decided to use cyber capabilities to assist in their strikes against Georgia. The use of cyber within the Russia-Georgia conflict is significant because it displayed the first successful use of synchronizing and integrating cyber effects into traditional kinetic operations. In David Hollis' "Cyberwar Case Study: Georgia 2008" he delves into the importance of the Russians being able to successfully target specific locations and organizations with cyber capabilities to aid in the success of the kinetic operations. In a similar manner to the attacks on Estonia, the Russians targeted Georgian government IT systems, civilian telecom systems, and news sites. While the world already knew that they possessed the capabilities to attack through the cyberspace domain, this was the first

time anyone had synchronized denial of service attacks to ensure that incoming strike packages reached their intended targets with little to no resistance[18]. The Russians managed to embarrass the Georgian government and let the rest of the world know that cyberspace is a valuable military asset and it was not to be taken lightly.

While the Russians proved that cyberspace could be used as a force multiplier, they still used it as an information operation which acted as an accessary to other strikes. In 2010 the idea of cyber being used for only information operations changed with the discovery of the STUXNET worm. Instead of attempting to execute a denial of service attack like many other worms or viruses before it, STUXNET instead targeted programmable logic controllers, which are devices that interact directly with machinery or hardware in order for them to execute a physical task.[19]

Muir S. Fairchild Research Information Center
Digital Collections
Air University–Maxwell AFB, AL

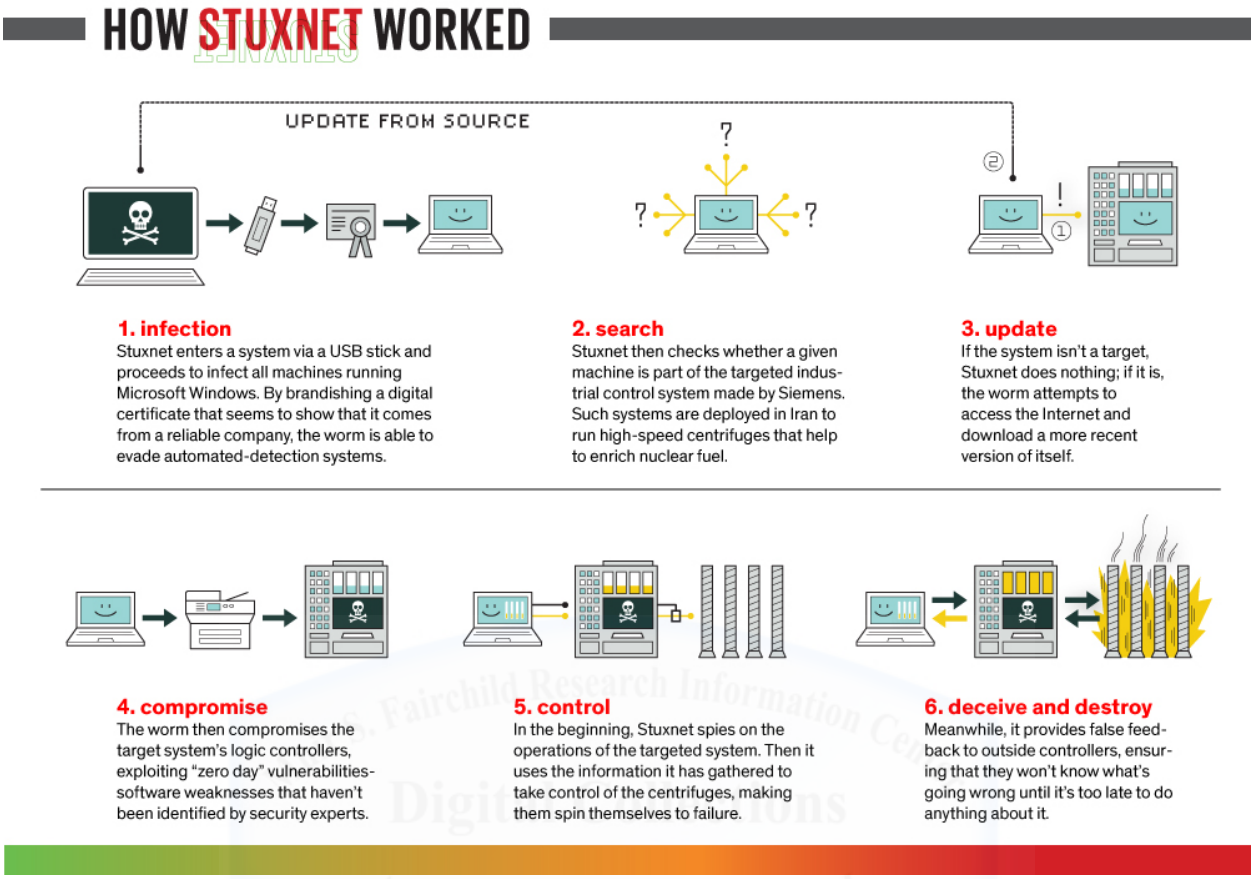

FIGURE 1: ILLUSTRATION OF THE HOW STUXNET PERFORMS[20]

This was essentially the first time that the world had seen a capability that originated in cyberspace have a physical effect similar to a kinetic operation. The most notable use of the STUXNET worm was an infection of the Iranian nuclear facilities in 2010. The worm was designed to attack a very specific piece of equipment which controlled the rate at which the Iranian centrifuges would spin. Once the network was infected and the exploit reached the hardware devices, it increased the spin of the centrifuges to a point where they would fail.[21] Even though STUXNET was designed to affect a very specific piece of equipment that was running a very specific version of software, it served as a proof of concept that offensive cyber operations could now provide effects similar to kinetic operations without having to penetrate hardened

facilities or putting personnel in harm's way. It also identified a major vulnerability in networks across the world as supervisory control and data acquisition (SCADA) systems, similar to the ones attacked in Iran, are used worldwide to perform tasks such as traffic control, managing power grids and management of other utility systems. The heavy reliance on SCADA systems and the effectiveness of STUXNET prompted former Secretary of Defense Leon Panetta to warn that the United States was now vulnerable to a "cyber Pearl Harbor".[22]

The last type of scenario that will be explored in this research deals with the recent hacks of the United States Office of Personnel Management (OPM) as well as attacks against the U.S. financial sector. In 2015 the Office of Personnel Management was discovered to have been hacked on two separate occasions and sensitive personnel records of over 20 million federal workers were exploited. Analysis of the hacking incidents linked the attacks back to groups with potential ties back into the Chinese Government. While the theft of personnel records is likely to be viewed more as an intelligence gathering operation than a cyber-attack, it brings up the questions of when does an exploit used for intelligence begin performing an offensive wartime function and when are attacks on civilian infrastructure, which can be attributed to a foreign government, an act of war? Gathering intelligence is nothing new to national security but with the continued development of cyber capabilities, what would once require you to essentially steal a safe or filing cabinet now requires the exploit of a server which can be done from almost anywhere in the world. In the case of the OPM hacks the amount of information obtained by the Chinese actors would have previously required someone to have infiltrated our sovereign borders and gained access to government facilities. It's not out of the question that that situation has occurred however the cyber domain now makes that situation exponentially more likely to happen. Media reports site that the Chinese groups responsible for the hack are compiling that

information into a very large database of federal employees that carry security clearances. [23] On the surface this looks like an extremely successful counter-intelligence operation, however what happens if the information retrieved in the hacks, leads to offensive operations against those individuals? Within cyberspace you will hear the term "selectors" used to describe pieces of information that form someone's virtual identity. Selectors can be phone numbers, IP addresses, physical addresses, social security numbers or anything else that you might use to identify an individual. During the hacks of the OPM database, the Chinese were able to obtain a variety of selectors for the individuals in the database. This will likely lead to increased collection by the Chinese against the individuals that they believe to have access to classified or sensitive material but the same accesses and exploits used to pull back information could be used to disrupt those individuals personal lives by affecting their finances, credit and other factors that impact daily life. In addition to using those selectors for collection, potentially harmful situations could occur if that information were sold to a group such as ISIS who have shown an intent to identify and publicly harm government and DOD employees. While the cyber operation may not be what physically harms the civilians affected, the potential exists for it to directly enable physical actions against the federal employees contained in the database.

Current International Cyber Agreements

The OPM hacks are the most current example of government sponsored hackers attacking non-military targets, however attacks on banks have been an ongoing problem over the last few years. Earlier this year, Kaspersky Labs identified that a hacking group conducted cyberattacks over the course of two years against various banks worldwide which ended up costing the affected organizations over one billion dollars.[24] The attacks could not be directly attributed to foreign government entities however they did identify a major vulnerability. In instances when

attacks are not attributed to government organizations, the government in the country where the attack originated may be asked to assist in identifying the infrastructure used for the attack and the individuals responsible, typical to counter-terrorism agreements that exist. Recently President Obama hosted Chinese President Xi Jinping and it was decided that the United States and China will come to an agreement on cooperation within cyberspace.[25] The agreement will include provisions prohibiting the cyber-enabled theft of intellectual property and trade secrets as well as agreements on how to cooperate with each other when cyber-crimes originate from within each country and a formal recognition of the 2015 United Nations report on acceptable behaviors within cyberspace.[26] Both countries are assigning delegates to participate in this joint dialogue and a hotline will be created between the delegates in order to quickly react to cyber issues that may occur. While this appears to be a step in the right direction, cyber operations can still operate in a very similar manner to terrorism operations in that attribution can be very difficult and it will be hard to verify whether China is operating in total accordance with this agreement.

In July 2015 the United Nations published a report titled "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" which identifies acceptable behaviors within cyberspace as well as ways for nations to further cooperate in order to help mitigate cyber threats against critical infrastructure.[27] The UN Secretary-General describes the importance of the document in his forward to the report;

> "Few technologies have been as powerful as information and communication technologies (ICTs) in reshaping economies, societies and international relations. Cyberspace touches every aspect of our lives. The benefits are enormous, but these do not come without risk. Making cyberspace stable and secure can only be achieved through international cooperation, and the foundation of this cooperation must be international law and the principles of the UN

> charter….Our efforts in this realm must uphold the global commitment to foster an open, safe and peaceful internet. In that spirit, I commend this report to the General Assembly and to a wide global audience as a crucial contribution to the vital effort to secure the ICT environment." [28]

This report appears to be one of the first international documents to attempt to apply international and humanitarian law to the use of information technology systems and it was written by experts from 20 different nations, including the United States, United Kingdom, Russia, and China. The document addresses views on how international law applies to the use of information technology systems. The first view is that "states have jurisdiction over the ICT infrastructure located within their territory."[29] This view is important because it reaffirms the idea of state sovereignty by allowing the country where equipment resides to maintain initial control of the use of the equipment. This statement will likely require further legal interpretation as most ICT systems are distributed throughout the world but it is as least a start by recognizing that nations have some level of control over things that reside within their boundaries. The second view identified within the report again deals with sovereignty and states that "states must observe, among other principles of international law, State Sovereignty, sovereign equality, and the settlement of disputes by peaceful means." also " states must "respect and protect human rights and fundamental freedoms."[30] This statement is especially important because of the lack of clear physical borders in cyberspace. As mentioned above, networks can be distributed all across the world and the days of looking at a map to identify someone's sovereign territory or property is no longer valid. The networks within the DOD are a perfect example of this. It is easy to state that we own the ICT equipment at our bases stationed across the world, but what about the transport networks that interconnect everyone. In some cases we may own the equipment from

end to end and can definitely say that it is our property but there are also times when we have to lease capacity from local telecommunication providers to ensure we can tie back into our networks back here in the United States. The second part of that statement that deals with respecting and protecting human rights and fundamental freedoms appears to be a direct attempt to state that the items outlined in the Geneva Convention in regards to humanitarian law are applicable in the cyber domain. While this is one of the first documents, recognized by the west as well as Russia and China, to officially begin to link cyber back to existing treaties and international agreements, the wording is still vague and does not provide the specificity required to accurately describe operations in cyberspace. The document does not describe any means of enforcing the policies outlined within it and it describes the intent of the report as "recommendations for consideration by the States for voluntary, non-binding norms, rules or principles of responsible behavior of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment."[31] The ideas contained within the report are guiding the international community in the right direction; however until it this becomes a binding legal agreement between States with clearly defined repercussions for failure to abide by the agreement, it will continue to be looked at as guidance instead of law.

While the United Nations document mentioned above described how everyone should cooperate in cyberspace using vague legal references and interpretations, a document published through the NATO Cyber Center of Excellence, titled the "Tallinn Manual" takes things one step further and directly applies the legal aspects of the Geneva Convention and other treaties to the world of cyberspace. The Tallinn Manual is named after the city of Tallinn which is the capital of Estonia. As stated in the case study on the Russian attacks on Estonia in 2007, Estonia was the most wired or networked country in the world at that time and it ended up falling victim to one

of the first successful large scale cyber-attacks against a State government, leading to Estonia being designated as the site of the Cyber Center of Excellence. The biggest difference between the United Nations document and the NATO document is that the NATO document is written by legal experts where the United Nations document was written by cyberspace professionals and the NATO document was written by western nations and does not appear to have input from nations such as China or Russia. The Tallinn Manual begins by focusing on sovereignty and jurisdiction just as the UN document did, however it expands its definitions to include situations that may occur during actual conflict. The Tallinn Manual expands the definition of sovereignty from an idea that a State maintains control over its physical boundaries to include a statement identifying that "A cyber operation directed by a State directed against the cyber infrastructure in another State, may violate the latter's sovereignty. It certainly does so if it causes damage."[32] In addition to defining sovereignty in regards to cyber operations, the manual also defines the legal recourse that States may take when their sovereignty is violated. Rule one section seven states:

> "If such cyber operations are intended to coerce the government (and are not otherwise permitted under international law), the operation may constitute a prohibited intervention or a prohibited use of force (Rules 10 to 12). A cyber operation that qualifies as an armed attack triggers the right of individual or collective self-defense (Rule 13). Actions not consulting an armed attack but are nevertheless in violation of international law may entitle the target State to resort to countermeasures (Rule 9). Security Council mandated or authorized actions under Chapter VII of the United Nations Charter (Rule 18), including those involving cyber-operations, do not constitute a violation of the target State's sovereignty."[33]

Each of the rules identified in the statement above, contain clearly defined responses that are acceptable when those situations present themselves. For instance Rule 13, Section 4 identifies that cyber operations that result in effects that would be considered analogues to

kinetic effects, that due to their scale would qualify as armed attacks, would be considered an armed attack and that the State that was attacked has the right to self-defense. [34] The authors of the manual went on to clarify that "any use of force that injures or kills persons or damages or destroys property would satisfy the 'scale and effects' requirement and would constitute an armed attack."[35]

In addition to the definitions of sovereignty and violations of sovereignty, the manual attempts to take the definition of civilians and civilian property from Article 52 of the Additional Protocols to the Geneva Convention and further clarify it in regards to cyberspace. The manual's definition of civilian objects and military objects is almost exactly the same as what is written in the Geneva Convention and reads: "Civilian Objects are all objects that are not military objectives. Military objectives are those objects which by their nature, location, purpose or use, make and effective contribution to military action…..Military objectives may include computers, computer networks and cyber infrastructure."[36] If something were to qualify as a military objective the manual goes on to state that before it is attacked, the intended effect must be definite and able to be controlled in order to prevent catastrophic second and third order effects. Rule 43 "prohibits means or methods of cyber warfare that indiscriminate by nature. Means and methods of cyber warfare are indiscriminate by nature if they cannot be: directed at a specific military objective, or limited in their effects as required by the law of armed conflict and consequently are of a nature to strike military objectives and civilians or civilian objects without distinction." [37] This statement is again almost taken verbatim from the Geneva Convention however the fact that it is restated as explicitly applicable to cyber warfare is a step in the right direction. In kinetic operations it is no longer common practice to bomb entire cities with the intent of striking one person or small group. We have seen this is counter-insurgency operations

where we send operators around looking for targets of interest while disturbing the civilian population as little as possible. Once a target is identified those small groups can strike or small precision strike munitions are used. This type of idea is no different when it comes to cyberspace. According to the Tallinn Manual, the capability used against the military objective must be vetted to the point where the operators know how it will reach the target and what it is designed to attack. It would not be good practice to turn loose an exploit that once you give the command to execute, you no longer have control over what it exploits or attacks.

The Tallinn Manual also addresses the release of dangerous forces through an attack on dams, dykes, and nuclear generator facilities similar to the Geneva Convention with the only addition being the addition of supporting computer networks to the definition. Rule 60 Section 6 states: "this Rule is confined to dams, dykes, nuclear electrical generating stations, and military objectives located in their vicinity, as well as to computers and computer networks that form an integral part of and support the operations of such works or installations."[38] This wording of this statement is important because it would be directly applicable to the STUXNET situation where the PLC controllers on the centrifuge were the subject of the attack and while those facilities were believed to be used for military purposes, there was no information to prove it and the attackers were never officially determined.

The Tallinn Manual appears to be the closest thing available to a "cyber Geneva Conventions document" and in a lot of cases the manual uses the exact same definitions as the Geneva Convention and expands it to include an application in the cyber domain. The only problem that may prevent this document from ever being adopted as a binding legal agreement was that there isn't any input from any of our adversarial nations. Without input from those

nations and the fact that one of the reviewers of the document is part of USCYBERCOM the odds of this being agreed to are not good.

Muir S. Fairchild Research Information Center
Digital Collections
Air University–Maxwell AFB, AL

Analysis, Conclusions and Recommendations

Analysis

The criteria the current cyber related agreements will be evaluated against are based on the general warfare documents identified above. The Geneva Convention and its Additional Protocols have been an international standard when it comes to warfare. The ideas of *Jus ad bellum* and *Jus in bello* ensure that war is somewhat regulated and that harm to parties not involved in the conflict is mitigated to the extent possible. While offensive cyber operations may not have the same direct effect on the population that chemical or nuclear weapons, we have seen where it can potentially have similar indirect effects in a situation such as the STUXNET attack on the Iranian nuclear facilities. In order to analyze the effectiveness of the current guidance in regards to cyber warfare, the documents will be evaluated against whether; they are enforceable, the current language is clearly applicable to the cyber domain or does it leave a lot to interpretation, is the language in line with the traditional warfare guidance in regards to *Jus ad bellum* and *Jus in bello* and is the document agreed upon by the major actors in cyberspace.

The ability to apply and enforce the current guidance is potentially the most problematic issue when it comes to cyberspace. In order to enforce the documents, a governing body must be able to attribute an attack or violation to a particular State or actor. Attribution within cyberspace is sometimes very hard to determine. In kinetic operations we typically have a good understanding of the types of equipment a nation has at their disposal and there are troop movements or launches that are observable in through intelligence means. In cyberspace an exploit may be installed and sit dormant and undiscovered until it receives an execution command with no one knowing that it existed until it was too late. In addition to its ability to ability to move stealthily through networks, cyber operations do not require a lot of capital to complete and can be executed by essentially anyone with a computer and a network connection.

The fact that an IP address can be traced back to adversarial country, does not guarantee that it was a State sponsored attack. This was the case in the Russia- Estonia cyber-attacks where the Russian government was likely involved but the attacks could not be directly attributed to government systems.

Of the documents examined in this research, the only document that is currently enforceable is the Geneva Convention and the additional protocols. It is the only document that is currently international law and is enforced by the UN charter. The UN document identifying acceptable behaviors in cyberspace helps expand a little on the Geneva Convention however it clearly states "recommendations for consideration by the States for voluntary, non-binding norms, rules or principles of responsible behavior of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment"[39]. It becomes very difficult to enforce something that is described as voluntary and non-binding. Enforcement of the Tallinn Manual may also be difficult but because of a different reason. The Tallinn Manual is written as a legal document such as the Geneva Convention, however in its current form it is just a research paper by NATO legal experts. If the Tallinn Manual were to be signed and agreed upon by the international community it would likely be enforceable and be just as effective as the Geneva Convention, if not more, due to its more current language.

When it comes to whether the language within the documents is applicable to operations in cyberspace, there appears to be different interpretations between different nations. The wording of the Geneva Convention is written in a manner for it to be applied to the types of warfare that were ongoing at the time. Passages pertaining to the use of nuclear, chemical and biological weapons are worded in a manner that leaves little up for interpretation while the definitions of civilians and civilian objects were left more vague and open to interpretation. As

mentioned above these definitions were written when warfare was only known to exist in the physical domains of air, land, sea and space. The creation of the man-made domain of cyberspace came well after these documents were drafted and while the wording was initially vague enough to be applicable to specific types of operations in cyberspace, the overall applicability is marginal at best. In the attacks against Estonia, systems that were used primarily for civilian emergency services were affected, and even though kinetic operations never occurred, this could have been determined to be in violation of international law by some States. In addition to Estonia, the Russian attacks on Georgia would have been considered more in line with the wording in the Geneva Convention as well as the expanded wording in the Tallinn Manual. The attacks were precise and required accesses that would have been developed well in advance of the execution of the operations. Even though civilian infrastructure was affected in this case, the attacks did not cause permanent damage and were controlled in a manner where it is unlikely that anyone would consider it an indiscriminant attack as defined in the Tallinn Manual. From a language applicability standpoint, the Tallinn Manual and the Geneva Convention will be almost identical due to the authors of the Tallinn Manual modeling the document off of the Geneva Convention. Of the three major documents described, the worst document in regards to the applicability of language is the United Nations document. It does not contain any clear definitions of what is expected other than that there is now an official recognition that everyone must now cooperate in cyberspace. The most important language within the UN document is in regards to maintaining an open and stable internet, which is likely one of the reasons that the US and other western States agreed to it. The UN description of the document identifies that it is based off of initial attempts by Russia as well as some of the other Caucus States to adopt an information security resolution, however early attempt at those

proposals failed due to concerns over States using the resolution as a means of restricting civilian use of the networks.[40] For that reason it appears that the statement "promoting an open, secure, stable, accessible and peaceful ICT environment" is likely the first step in UN States forming a gentlemen's agreement that further legal agreements will take the availability of ICT systems to civilians into account.[41]

The argument of whether the current documents are consistent with the underlying themes of *Jus in Bello* and *Jus ad Bellum* is heavily reliant on the language discussed above. The Geneva Convention is obviously going to uphold the themes since it is essentially the guide for describing the legal reasons to declare war or begin a conflict (*Jus ad Bellum*) and how to regulate conflict once it has begun (*Jus in Bello*).[42] Due to the inclusion of most of the Geneva Convention language, the Tallinn Manual is written in a manner that inherently includes those underlying tenets of international warfare law. The language within the Tallinn Manual, due to its expanded Geneva Convention definitions attempting to include cyberspace, may actually be the most comprehensive of the documents because it attempts to cover the current nuances of civilian cyber systems being used by military and even non-state actors. As identified in the description of the Tallinn Manual above, it outlines specific current situations regarding when a State has the authority to retaliate for a strike as well as the extent of the retaliation. Both the Geneva Convention but more so Tallinn Manual could be applied to the Russia-Estonia attacks, Russia-Georgia Attacks, the use of STUXNET, and the OPM hacks and provide enough guidance to come up with a legal interpretation of the validity of the strikes. While there is really no argument against the fact that the Geneva Convention and the Tallinn Manual are consistent with *Jus in Bello* and *Jus ad Bellum*, the same cannot be said for the United Nations document. As mentioned above the language within the United Nations document is vague and does not

really provide clear guidance in regards to either principle. The UN document appears to be geared more towards coming to an understanding on the cooperative use of cyberspace and not on regulating how it would be used in a wartime situation. Of the situations described in the literature review, the Russian attacks on Estonia and the OPM hacks are really the only two that this document may loosely apply to. Paragraph 13(c-f) states that states shouldn't knowingly allow their infrastructure to be used for wrongful acts against other states and if a wrongful act involving State ICT systems occurs, the States are to cooperate in the investigation to attempt to find the criminal or terrorist who executed the attack.[43] Paragraph 13(f) could potentially apply to the STUXNET attack against the Iranian nuclear facilities however it would be a bit of a stretch as the rule states: "A state should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public."[44] Assuming the Iranian claims that the nuclear sites are for peaceful purposes and serve no military function, the situation could be interpreted as violation of that paragraph, however due to its lack of enforceability; there would be no repercussion for any violation.

The last criteria used to evaluate the effectiveness of the current warfare guidance in regards to cyber operations is whether the documents have been agreed upon by the international community. For any type of guidance to be effective, it must be acknowledged and agreed upon by those who intend to follow it. This metric is very similar to the enforceability metric discussed above but is different enough to evaluate on its own because something must be agreed to before it can be enforced. The Geneva Convention is by far the most effective in regards to this metric because it has been the agreed upon standard for decades and even centuries for some provisions within it. The document has been agreed to by countries that are part of the United

Nations including most of the nations we would consider to be adversaries, such as Iran, China Russia and North Korea. In every one of the scenarios identified in the literature review, the situation would have been compared to the Geneva Convention in order to determine if there was a violation of international law. In some cases the lack of attribution made it difficult to determine who was at fault and potentially committed a violation but that could be due to a lack of wording that pertains specifically to situations that occur within cyberspace. A document that could help mitigate issues of vague wording in regards to cyberspace is the Tallinn Manual. The issue with the Tallinn Manual is that it is currently not an agreed upon international agreement like the Geneva Convention. The Tallinn Manual is sponsored by NATO nations and even if it were recognized as international law by those nations, there would only be 28 nations agreeing to it instead of the 193 nations that are part of the United Nations. [45] [46] Even though the language is consistent with the Geneva Convention it may still take some time before something like this is agreed upon by the entirety of the United Nation's states. In a similar situation to the Tallinn Manual, the United Nations document on acceptable behaviors in cyberspace is not currently an agreed upon legal document. It was developed by experts from States that are members of the United Nations, however only experts from 20 of the 193 States participated. [47] The document has a long way to go before being considered a legally binding document and considering it is only 17 pages in length, it wouldn't even come close to covering the amount of material contained in the Tallinn Manual or the Geneva Convention. While it is a good step forward that nations are voluntarily agreeing to its concepts, this document is likely to be combined or act as a precursor to an eventual agreement that will be adopted by the United Nations in the future.

Conclusions

After analysis of the effectiveness of the current warfare guidance in regards to cyber operations a few conclusions become apparent. For one of the documents to be as effective as possible it must be enforceable, agreed upon by the international community, contain language consistent with today's technology on the battlefield and remain consistent with the principles of *Jus in Bello* and *Jus ad Bellum.* The Geneva Convention and all of its additional protocols have been the standard for decades and are in compliance with most of the criteria above. Where the Geneva Convention begins to fall short is the lack of language consistent with the use of the cyber domain and the application of *Jus ad Bellum* to cyber operations. The Geneva Convention does a good job of describing a state's sovereignty and when retribution for an act that violates that sovereignty is warranted. The issue with that definition being applied to today's use of cyberspace is that the definition is meant to be applied to acts that occur on air, land or sea. When this document was written, it was very easy to see when someone had crossed into someone else's territory and invaded their sovereign land. In today's fight similar to the situation between Estonia and the Russian cyber actors, someone can attack you from outside your borders with something that you will not see coming at you in the air, land and sea domains. In traditional warfare operations or strikes you will hear the term "proportional response" for when violations of a state's sovereignty are threatened, but there is no clear definition of how to deal with strikes that occur in cyberspace. The STUXNET attacks on the Iranians cause physical damage to their systems but due to the lack of legal precedence for this type of situation, as well as a lack of attribution, they had no guidance as to how they could respond. The Geneva Convention is enforceable, it is the agreed upon standard, and for the most part it does a good job of covering the majority of warfare within its language.

The Tallinn Manual is shown to have been based off of the Geneva Convention. It uses the exact same language in most of the sections and includes additions that cover the situations that the language in the Geneva Convention could not. Paragraphs within the manual could be directly applied to every one of the scenarios identified in the case studies. The addition of language related to cyber builds on the foundation set by the Geneva Convention and creates a document that is applicable across all domains on today's battlefield. The shortfalls in the Tallinn Manual are not contained within its text but rather in its current form as a NATO sponsored research paper. Because it is not an agreed upon legal document is in no way enforceable throughout the international community.

The UN document is by far the weakest of the three documents after it was evaluated against the criteria. The language within the document tries to highlight some of the more important principles such as sovereignty and jurisdiction in cyberspace but the wording was vague and left quite a bit up for interpretation. While the document was touted as a major step forward in cooperation within cyberspace, it does not come close to covering the aspects of cyber that are covered within the Tallinn Manual. The UN document also makes no attempt at covering any of the traditional warfare guidance from within the Geneva Convention and almost appears as though it was thought to be used as an addendum to the Geneva Convention for cyber. The biggest success with this document is obtaining the initial gentlemen's agreements that cyberspace is supposed to remain free and secure. Initial attempt at adopting resolutions failed due to the belief that State's would begin regulating the internet to a point where the civilians would no longer have stable and secure access. While this is a major step in the right direction from that standpoint, this document will never become the agreed upon standard for today's warfare, unless it is substantially updated.

Recommendation

Based on the conclusions above, the adoption on the Tallinn Manual would be the recommended course of action. The document contains the tradition language within the Geneva Convention as well as updated language to accurately reflect today's battlespace. The Geneva Convention could be considered effective at covering almost all aspects of war except for some of the nuances presented in cyberspace. Those nuances are exactly what the Tallinn Manual intends to add to the language within the Geneva Convention and if it were adopted it would be a comprehensive guide to regulate the reasons that warrant retribution or conflict (*Jus ad Bellum*) as well as how to regulate actions once conflict has begun (*Jus in Bello*). Adoption of this documents may require additional agreement such as the United Nations document on acceptable behaviors in cyberspace to be legally adopted as well to ensure that all parties acknowledge the fact that access to cyberspace and the internet is to be recognized as a basic right of civilians across the world. We are likely a few years or a catastrophic event away from the adoption of these documents but it something that is an eventual necessity. The initial Geneva Conventions were written in 1949 with additional protocols published in 1977 and 2005.[48] Based on that trend of updates there is likely to be another attempt at updating the document in the next 15 years, however with the speed at which technology progresses it is likely that the update will come sooner.

Digital Collections

Notes

[1] Threat analysis of the WCIT part 4: The ITU and Cybersecurity. Retrieved May 30, 2015, from http://www.internetgovernance.org/2012/06/21/threat-analysis-of-the-wcit-4-cybersecurity/
[2] Foreign Policy Cyber Security. Retrieved May 31, 2015, from https://www.whitehouse.gov/issues/foreign-policy/cybersecurity
[3] Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*. Jan 60, 211.
[4] Herzog, S. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. Journal of Strategic Security, 49-60.
[5] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. https://www.icrc.org/ihl/WebART/470-750067
[6] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1), Geneva, 8 June 1977, Article 85(3)(c). https://www.icrc.org/customary-ihl/eng/docs/v2_rul_rule42
[7] Zetter, Kim. "An Unprecedented look at STUXNET, the World's First Digital Weapon". Wired.com. 3 November 2014. http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
[8] Markoff, J., & Kramer, A. (2009, June 27). "U.S. and Russia Differ on a Treaty for Cyberspace." *New York Times* Retrieved June 20, 2015. http://www.nytimes.com/2009/06/28/world/28cyber.html?_r=0
[9] Grigsby, A. (2015, January 28). "Will China and Russia's Updated Code of Conduct Get More Traction in a Post-Snowden Era?" *Council on Foreign Relations*.Retrieved June 15, 2015. http://blogs.cfr.org/cyber/2015/01/28/will-china-and-russias-updated-code-of-conduct-get-more-traction-in-a-post-snowden-era/
[10] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. Article 52. https://www.icrc.org/ihl/WebART/470-750067
[11] Ibid.
[12] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1), Geneva, 8 June 1977, Article 56
[13] Ibid.
[14] Law of Armed Conflict Deskbook. International and Operational Law Department, The United States Army Judge advocate General's Legal Center and School. Charlottesville VA. 2012
[15] Herzog, S. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. Journal of Strategic Security, 49
[16] Ibid. 49
[17] Ibid. 49
[18] Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*. Jan 60, 211.
[19] Chen, Thomas M. "Stuxnet, the Real Start of Cyber Warfare?" *IEEE Network*. 2010
[20] Kushner, David. "The Real Story of Stuxnet." *IEEE Spectrum. 2013*
[21] Ibid.
[22] Ibid.
[23] Wood, Todd. "Chinese Compiling 'Facebook' of U.S. Government employees". The Washington Times. 16 September 2015
[24] "Cyber attacks a growing threat for USS financial system". Phys.org. 20 May 2015. http://phys.org/news/2015-05-cyber-threat-financial.html
[25] The White House. "Factsheet: President Xi Jinping's State Visit to the United States". 25 September 2015. https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states
[26] Ibid.
[27] United Nations. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security". 22 July 2015. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

[28] United Nations Office for Disarmament Affairs. “Developments in the Field of Information and Telecommunications in the Context of International Security” http://www.un.org/disarmament/topics/informationsecurity/
[29] United Nations. “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security”. 22 July 2015. Page 12. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174
[30] Ibid. p 12
[31] Ibid. p. 7
[32] NATO Cooperative Cyber Center of Excellence. 2012. "Tallinn Manual Process." *NATO CCDCOE.* Accessed September 2015. https://ccdcoe.org/tallinn-manual.html. p 16
[33] Ibid. p 17
[34] Ibid. p 54
[35] Ibid. p 55
[36] Ibid. p 125
[37] Ibid. p 145
[38] Ibid. p 224
[39] United Nations. “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security”. 22 July 2015. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174
[40] Ibid. p 7
[41] Ibid. p 7
[42] Law of Armed Conflict Deskbook. International and Operational Law Department, The United States Army Judge advocate General’s Legal Center and School. Charlottesville VA. 2012
[43] United Nations. “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security”. 22 July 2015. P 8 http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174
[44] Ibid. P 8
[45] "United Nations Member States." *United Nations.org.* Accessed October 2015. http://www.un.org/en/members/index.shtml.
[46] "NATO Countries." *NATO.int.* Accessed October 2015. http://www.nato.int/cps/en/natolive/nato_countries.htm.
[47] United Nations. “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security”. 22 July 2015. P 8 http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174
[48] International Red Cross. “The Geneva Conventions”. https://www.icrc.org/en/war-and-law/treaties-customary-law/geneva-conventions

References

Chen, Thomas. 2010. "Stuxnet, the Real Start of Cyber Warfare?" *IEEE Network.*

Grigsby, A. 2015. "Will China and Russia's Updated Code of Conduct Get More Traction in a Post-Snowden Era?" *Council on Foreign Relations.* January 28. Accessed June 2015. http://blogs.cfr.org/cyber/2015/01/28/will-china-and-russias-updated-code-of-conduct-get-more-traction-in-a-post-snowden-era/.

Herzog, S. n.d. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Studies* 49-60.

Hollis, David. 2011. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal.*

International and Operational Law Department. 2012. "Law of Armed Conflict Deskbook." *The United States Army Judge Advocate Generals Legal Center and School.* Accessed May 2015.

International Red Cross. n.d. *The Geneva Conventions.* Accessed October 2015. https://www.icrc.org/en/war-and-law/treaties-customary-law/geneva-conventions.

InternetGovernance.Org. n.d. *Threat Analysis of the WCIT part 4: The ITU and Cybersecurity.* Accessed May 30, 2015. http://www.internetgovernance.org/2012/06/21/threat-analysis-of-the-wcit-4-cybersecurity/.

Kushner, David. 2013. "The Real Story of Stuxnet." *IEEE Spectrum.*

Markoff, J, and A Kramer. 2009. "U.S. and Russia Differ on a Treaty for Cyberspace." *New York Times*, June 28.

NATO Cooperative Cyber Center of Excellence. 2012. "Tallinn Manual Process." *NATO CCDCOE.* Accessed September 2015. https://ccdcoe.org/tallinn-manual.html.

n.d. "NATO Countries." *NATO.int.* Accessed October 2015. http://www.nato.int/cps/en/natolive/nato_countries.htm.

1977. "Protocal Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I)." *International Committee of the Red Cross.* June 8. Accessed September 2015. https:www.icrc.org/ihl/WebART/470-750067.

1977. "Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I) Article 56." *International Committee of the Red Cross.* June 08. Accessed September 2015. https://ircr.org/ihl/WebART/470-750067.

1977. "Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I), Article 85(3)(c)." *International Committee of the Red Cross.* June 08. Accessed September 2015. https://www.icrc.org/customary-ihl/eng/docs/v2_rul_rule42.

The White House. 2015. "Factsheet: President Xi Jinping's State Visit to the United States." *White House.Gov.* September 25. Accessed September 2015. http://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinping-sate-visit-united-states.

The Whitehouse. n.d. "Foreign Policy Cyber Security." *whitehouse.gov.* Accessed May 31, 2015. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity.

United Nations. 2015. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." *United Nations.org.* July 15. Accessed September 2015. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

n.d. "United Nations Member States." *United Nations.org.* Accessed October 2015. http://www.un.org/en/members/index.shtml.

United Nations Office for Disarmament Affairs. 2015. "Developments in the Field of Information and Telecommunications in the context of International Security." *United Nations.org.* July 22. Accessed September 2015. http://www.un.org/disarmament/topics/informationsecurity/.

Wood, Todd. 2015. "Chinese Compiling'Facebook' of U.S. Government employees." *Washington Times*, September 16.

Zetter, Kim. 2014. "An Unprecedented Look at STUXNET, the World's First Digital Weapon." *Wired.com.* November 3. Accessed May 2015. http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

Muir S. Fairchild Research Information Center
Digital Collections
Air University–Maxwell AFB, AL